Congressional Research Service
Informing the legislative debate since 1914

Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations

Updated July 2, 2015

Congressional Research Service
https://crsreports.congress.gov
R43604

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The U.S. electric power grid consists of over 200,000 miles of high-voltage transmission lines and hundreds of large transformer substations. High voltage (HV) transformer units make up less than 3% of U.S. transformers, but they carry 60%-70% of the nation's electricity. Because they serve as vital nodes, HV transformers are critical to the nation's electric grid. HV transformers are also the most vulnerable to damage from malicious acts.

For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures. There has been some level of physical security investment and an increasing refinement of voluntary security practices across the electric power sector for at least the last 15 years. However, recent grid security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have changed the way grid security is viewed and have focused congressional interest on the physical security of HV transformers. They have also prompted new grid security efforts by utilities and regulators.

On November 20, 2014, the Federal Energy Regulatory Commission (FERC) approved a new mandatory Physical Security Reliability Standard (CIP-014-1) proposed by the North American Electric Reliability Corporation (NERC). The new standards require certain transmission owners "to address physical security risks and vulnerabilities related to the reliable operation" of the power grid by performing risk assessments to identify their critical facilities, evaluate potential threats and vulnerabilities, and implement security plans to protect against attacks. Legislative proposals would expand federal efforts to prevent or recover from a physical attack on the U.S. grid. These include the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243).

There is widespread agreement among government agencies, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the actual risk of a multi-HV transformer attack remains an open question. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several issues as part of its oversight of the sector: identifying critical transformers, confidentiality of critical transformer information, adequacy of HV transformer protection, quality of federal threat information, recovery from HV transformer attacks, and the overall resiliency of the grid. Maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

Contents

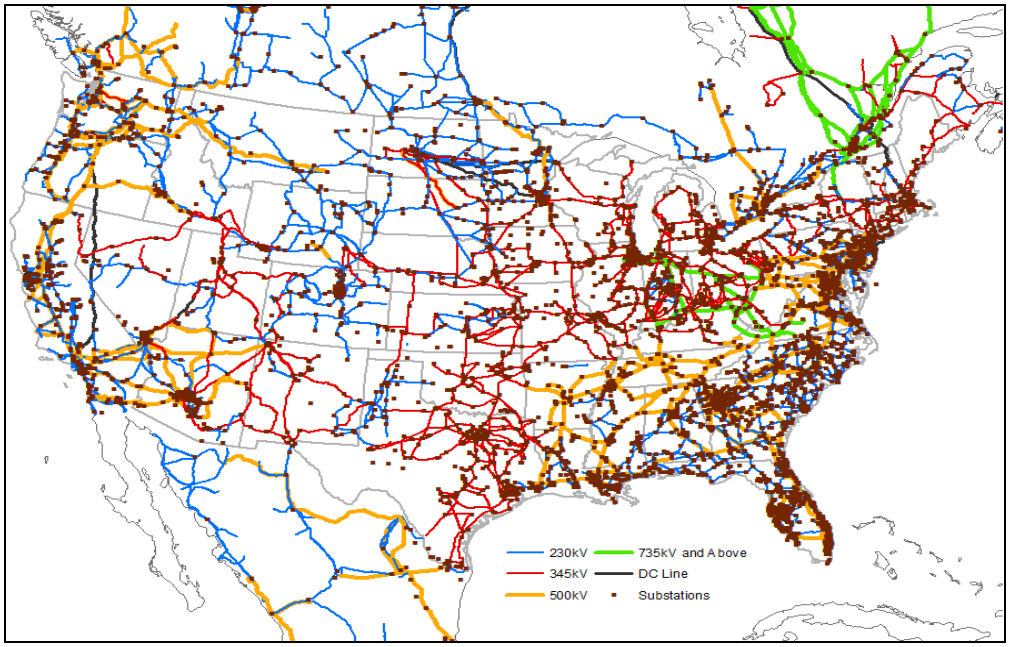
Figures

Contacts

Introduction[1]

The electric utility industry operates as an integrated system of generation, transmission, and distribution facilities to deliver electric power to consumers. In the United States, this system consists of over 9,000 electric generating units connected to over 200,000 miles of high-voltage transmission lines strung between large towers and rated at 230 kilovolts (kV)[2] or greater.[3] This network is interspersed with hundreds of large electric power transformer substations whose function is to adjust electric voltage as needed to move power across the network (**Figure 1**). High voltage (HV) transformer units make up less than 3% of transformers in U.S. power substations, but they carry 60% or more of the nation's electricity.[4] Because they serve as vital transmission network nodes and carry bulk volumes of electricity, HV transformers are critical elements of the nation's electric power grid.

Figure 1. Electric Transmission Network



Sources: CRS analysis of GIS data from Platts, HSIP Gold 2013 (Ventyx), and Esri.

[1] Portions of this report were drawn from CRS Report R42795, *Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism*, by Amy Abel, Paul W. Parfomak, and Dana A. Shea.

[2] 1 kV=1,000 volts.

[3] North American Electric Reliability Corporation, "Understanding the Grid," fact sheet, August 2013, http://www.nerc.com/AboutNERC/Documents/Understanding%20the%20Grid%20AUG13.pdf. Note that there is no industry consensus as to what voltage rating or other operating characteristic constitutes "high voltage." This report uses 230 kV as the high voltage threshold, but other studies may use a different threshold, such as 115/138 kV, or may include an additional "extra high voltage" category above 345 kV. See, for example, U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid*, April 2014, p. 4.

[4] C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997; William Loomis, "Super-Grid Transformer Defense: Risk of Destruction and Defense Strategies," Presentation to NERC Critical Infrastructure Working Group, Lake Buena Vista, FL, December 10-11, 2001; Electric Power Research Institute (EPRI), *Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry*, prepared for the U.S. Department of Homeland Security, September 30, 2014, p. 13.

The U.S. electric power grid has historically operated with such high reliability that any major disruption caused by weather, operational errors, or sabotage, makes news headlines. The various parts of the electric power system are all vulnerable to failure due to natural, operational, or manmade events. Such outages can have considerable negative impacts on business, government services, and daily life. Notwithstanding its high reliability overall, the U.S. power grid has periodically experienced major regional outages. Recent examples include the Northeast Blackout of 2003 (which affected 55 million customers in eight states and Canada) and extended outages in the New York/New Jersey area after Superstorm Sandy in 2012. For reasons discussed below, however, HV transformers are considered by many experts to be the most vulnerable to intentional damage from malicious acts. The physical security of HV transformers and associated policy issues are the subject of this report.

Congressional Interest

Congress has long been concerned about grid security in general, but recent security exercises, together with a 2013 physical attack on transformers in Metcalf, CA, have focused congressional interest on the physical security of HV transformers, among other specific aspects of the grid.[5] They have also prompted new grid security initiatives by utilities and federal regulators. Legislative proposals including the Enhanced Grid Security Act of 2015 (S. 1241), the Critical Electric Infrastructure Protection Act (H.R. 2271), the Terrorism Prevention and Critical Infrastructure Protection Act of 2015 (H.R. 85), a House bill to establish a strategic transformer reserve program (H.R. 2244), and the Grid Modernization Act of 2015 (S. 1243) would expand these activities by strengthening federal efforts to prevent or recover from a physical attack on the U.S. grid.

HV Transformer Risks and Vulnerability

The main risk from a physical attack against the electric power grid—primarily towers and transformers—is a widespread power outage lasting for days or longer. Utilities regularly experience damage to transmission towers due to both weather and malicious activities; they are able to recover from this damage fairly rapidly. Thus, while occasionally causing blackouts, physical attacks on towers generally have not resulted in widespread or long-lasting outages. The power industry also has experienced mechanical failure of individual HV transformers within a single control area resulting in blackouts lasting hours. However, no region in the United States has experienced simultaneous failures of multiple HV transformers. Experts have long asserted that a coordinated and simultaneous attack on multiple HV transformers could have severe implications for reliable electric service over a large geographic area, crippling its electricity network and causing widespread, extended blackouts. Such an event would have serious economic and social consequences. This section discusses in more detail HV transformer characteristics and physical security risks associated with them.

High Voltage Power Transformers

Utility transformers control the voltage of electricity so that it can be synchronized with other power supplies, transmitted long distances, and distributed to customers. Transformers range in size from small, pole-mounted units that may serve a dozen homes to transmission units that

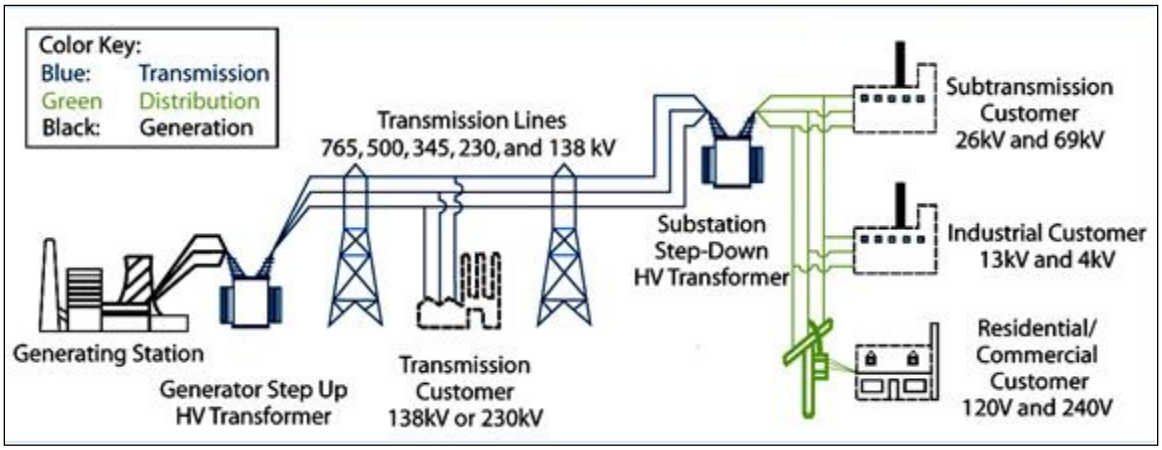
[5] See, for example: Senators Dianne Feinstein, Al Franken, Ron Wyden, and Harry Reid, letter to the Honorable Cheryl LaFleur, Acting Chairman, Federal Energy Regulatory Commission, February 7, 2014, http://www.ferc.gov/industries/electric/indus-act/reliability/chairman-letter-incoming.pdf.

serve an entire city. The larger the transformer, the higher the voltage the transformer can handle. Utility transformers, regardless of size, fundamentally consist of copper wire wrapped around a metallic "core" within an insulated protective housing covered with a 5/8 to 3/4-inch mild steel tank. They are linked to the power grid by protruding metal and (usually) ceramic connectors called "bushings" which resemble giant spark plugs. Larger transformers generate waste heat during operation (like all transformers), so they are cooled by a system comprised of internally circulating oil and external radiators, analogous to the cooling system in a car engine. Large transformers are located in network substations along with transmission lines, associated electric equipment, and system controls. These substations may be found in remote locations or near urban centers, depending upon regional transmission needs. Many are located alongside electric generation plants, linking those plants to the grid.

Voltage Management in the U.S. Power System

Electricity produced at U.S. generating stations is converted into a set of three alternating electric currents called three-phase power.[6] The first step in delivering this power is transforming it from the generated voltage (typically 15-50 kV) to higher voltage (138-765 kV), allowing transmission over long distances in greater volumes most efficiently (**Figure 2**).[7] This initial voltage step-up occurs by means of transformers located at transmission substations adjacent to the generating facilities. (The three phases of power are carried separately over three wires on transmission towers.) Close to the ultimate consumer, the power is stepped-down at another transformer substation to lower voltages, typically 13 kV or less. At this point, the power is considered to have left transmission and entered the local distribution system.

Figure 2. Step-Up and Step-Down HV Transformers in the Grid



Source: Adapted by CRS from: U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, Figure 2.1.

High-voltage transformers, especially units above 345 kV, are physically large and extraordinarily heavy. For example, **Figure 3** shows a new 345 kV transformer many times larger than the pickup

[6] The three currents are sine wave functions of time with the same frequency (60 Hertz). The phases are spaced equally, offset 120 degrees from each other. With three-phase power, one of the phases is always nearing a peak.

[7] The loss of power on the transmission system is proportional to the square of the current (flow of electricity) while the current is inversely proportional to the voltage.

truck parked alongside. This transformer unit weighs 435 tons, including 29,000 gallons of cooling oil.[8] (Note that the vertical bushings are not yet connected to transmission lines because the unit is being moved.) This is a three-phase unit, with one bushing for each of the three phases. Some substations alternatively employ separate single-phase transformers in sets of three. Generally, the higher the transformer's voltage, the larger the transformer. A three-phase 765kV transformer could be 45 feet tall and occupy a footprint of 2,200 square feet—about the size of an average new single-family house.[9]

Figure 3. Installation of a 345 kV Transformer

Source: Courtesy of Pauwels Canada, Inc., 2003.

Manufacture and Cost

Most HV transformers are unique—designed and manufactured to custom specifications for a specific network application. In 2010, the lead time between an HV transformer order and delivery ranged from 5 to 12 months for U.S. manufacturers and 6 to 16 months for foreign manufacturers, although lead times well over 20 months could be required in certain situations.[10] This process may include three to four months for the engineering design alone.[11] Since manufacturing generally occurs on a single production line with just-in-time component supplies, advanced production scheduling is important for managing delivery. Physical assembly is labor intensive, requiring manual winding of the copper wire around the transformer core and frequent engineering checks during manufacturing. Extensive testing of completed units also contributes to HV transformer manufacturing time.

The installed cost for an HV transformer depends heavily on its configuration and specific design requirements. New HV transmission substations can cost well in excess of $10 million, including

[8] Pauwels Canada, Inc., personal communication, October 20, 2003.

[9] U.S. Department of Energy, April 2014, p. 7.

[10] U.S. Department of Energy, April 2014, p. 9.

[11] Emily Heitman, ABB Inc, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power hearing entitled "Discussion Draft Addressing Energy Reliability and Security," May 19, 2015; Pauwels Canada, Inc., October 20, 2003.

the cost of transformers and other station equipment. According to the U.S. Department of Energy (DOE), the factory prices for HV transformers typically range from $2 million for a 230 kV unit to $7.5 million for a 765 kV unit, before transportation and installation costs.[12]

U.S. Manufacturing Capability

From 1950 to 1970, utility construction of large generation plants and associated transmission networks fueled a robust U.S. manufacturing market for large transformers. During this period, the United States (and Canada) accounted for approximately 40% of global demand for such units.[13] After 1970, however, utility investment in transmission infrastructure began falling off due to perceived overcapacity, public resistance to transmission siting, and greater regulatory scrutiny of capital expenditures. Beginning in the late 1980s, uncertainty about industry restructuring and the introduction of competition made grid owners even less willing to invest in new transmission. This decline in U.S. transmission investment greatly reduced domestic demand for large transformers, especially HV transformers. By the late 1990s, the United States and Canada accounted for only 20% of global large transformer sales.[14] Demand in the United States has subsequently increased, however. For example, between 2005 and 2013, the total value of large transformers (including medium- and high-voltage units) imported to the United States more than doubled, from $284 million (363 units) to $676 million (496 units).[15]

At the same time, global demand for transformers continued to grow and more foreign manufacturers entered the market. According to U.S. industry representatives, many of these foreign manufacturers benefited from dramatically lower labor costs, so they could underbid U.S. transformer makers for the remaining U.S. demand. Some of these foreign manufacturers may have been protected by import barriers which effectively closed their home markets to U.S. transformer imports. Today, there is limited manufacturing capacity in the United States for HV transformers. Five U.S. facilities state that they can manufacture transformers rated 345 kV or above, although it is not clear how many units in this range they have actually produced. Canada and Mexico have five additional HV manufacturing plants.[16] While limited domestic HV transformer manufacturing may increase delivery time, utilities have not reported difficulty in obtaining needed equipment.

HV Transformer Sites in the United States

There are several thousand HV transformers operating in the United States. Approximately 2,100 are very large units rated 345 kV and above.[17] Investor-owned utilities own most of these, although public utilities such as the Power Marketing Administrations (i.e., Bonneville Power Administration and Western Area Power Administration), Tennessee Valley Authority, and the Los Angeles Department of Water and Power own many HV transformers as well.[18] HV

[12] U.S. Department of Energy, April 2014, p. 7.

[13] C. Newton, "The Future of Large Power Transformers," *Transmission & Distribution World*, September 1, 1997.

[14] C. Newton, September 1, 1997.

[15] U.S. Department of Energy, April 2014, p. 27.

[16] Kenneth Friedman, U.S. Department of Energy, "DOE Update on GMD/EMP-Related Activities," Presentation to the Geomagnetic Disturbance Task Force Working Group, North American Electric Reliability Corporation, November 13, 2013.

[17] John Kappenman, *Geomagnetic Storms and Their Impacts on the U.S. Power Grid*, Meta-R-319, Metatech Corp., prepared for Oak Ridge National Laboratory, January 2010, p. 1-14, http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-319.pdf.

[18] HV substation information for specific investor-owned utilities is publicly available in annual reports filed with the Federal Energy Regulatory Commission (FERC Form-1).

transformer substations are distributed throughout the electric grid, as shown in **Figure 1**, with the greatest number in the eastern part of the country.

Criticality of HV Transformers

Because HV transformers carry so much electricity, the destruction of even a small number could seriously reduce the transmission capacity of a regional electric power grid and lead to extended blackouts. The impact of such a failure would depend on the electricity flows in that part of the grid, congestion from major network bottlenecks, and the status of other key facilities such as power plants, transmission lines, and other substations. Power grid planners generally anticipate the possible loss of a single HV transformer substation and are prepared to reroute power flows as necessary to maintain regional electric service. But the simultaneous loss of multiple HV transformers, especially in a constrained transmission area, could exceed the capability of a regional network to reroute power through secondary lines.[19]

Numerous publicly available studies have analyzed the risks from such a multiple failure. For example, the Congressional Office of Technology Assessment (OTA), in a 1990 report on the physical vulnerability of the electric power system, found that

> In most cases, the nearly simultaneous destruction of two or three transmission substations would cause a serious blackout of a region or utility, although of short duration where there is an approximate balance of load and supply.... The destruction of more than three transmission substations would cause long-term blackouts in many areas of the country.[20]

In such an emergency scenario, limited electric service could likely be restored in the short term by imposing "rolling" blackouts, rerouting transmission, and using portable transformers. Nonetheless, the loss of key HV substations would leave the regional network crippled and highly susceptible to further disturbance and cascading failure.[21] According to power industry experts, certain parts of the U.S. transmission network are particularly vulnerable to HV substation disruption. These areas may have severely constrained transmission paths relying on a small number of HV transformers in extremely critical network locations. According to press accounts, a FERC power flow analysis in 2013 identified 30 such critical HV transformer substations across the continental United States; disabling as few as nine of these substations during a time of peak electricity demand reportedly could cause a "coast-to-coast blackout."[22]

Notwithstanding the FERC study and similar claims by security analysts, the actual risk to the U.S. grid of extended blackouts due to a deliberate attack on multiple HV transformers is the subject of ongoing debate. An investigation by the Department of Energy's Office of Inspector General (IG) appears to discredit FERC's risk analysis. According to the IG investigation, officials at the department previously concluded that FERC's study was based on "highly unlikely assumptions" and that "loss of the critical substations identified in the analysis would not result in the consequence described in the analysis or any other consequence that could be reasonably expected to result in damage to national security."[23] Due to the complexity of HV

[19] National Research Council (NRC), *Terrorism and the Electric Power Delivery System*, 2012, p. 69; EPRI, September 30, 2014, p. 7.

[20] Office of Technology Assessment (OTA), *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, June 1990, p. 37.

[21] See, for example, Réka Albert, István Albert, and Gary L. Nakarado, "Structural Vulnerability of the North American Power Grid," *Physical Review E*, Vol. 69, 025103(R), 2004.

[22] Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack," *Wall Street Journal*, March 12, 2014.

[23] U.S. Department of Energy, Office of Inspector General, *Inspection Report: Review of Controls for Protecting*

transmission networks and uncertainties about potential physical threats, a range of differing conclusions may be reached by industry experts on the potential severity and duration of a blackout from a multi-transformer attack. However, most analysts acknowledge that severe regional, if not national, power outages may be technically possible under certain conditions.[24]

Physical Vulnerability of HV Transformers

The Department of Energy's recent *Quadrennial Energy Review* identifies HV transformers as one of the electric grid's "most vulnerable components."[25] All HV transformers are designed to withstand operational risks such as lightning strikes, hurricanes, and network power fluctuations—but they are vulnerable to intentional physical attacks. Despite their great size and internal complexity, HV transformers of conventional design can be readily disabled or destroyed. According to one manufacturer, "if someone were to intentionally try ... it is a surprisingly simple task and there are a large number of ways to conceivably damage a transformer beyond repair."[26] Transformer experts have asserted that a bad actor with basic knowledge of transformer design could inflict irreparable damage. Such attacks can cause massive electrical short circuits and oil fires that would destroy an HV transformer and damage surrounding infrastructure. One fire at a 345 kV substation in Texas, for example, destroyed the transformer and burned for five hours, causing "plumes of smoke that could be seen for miles."[27] In addition to direct attacks on the transformers themselves, HV substations can be further disabled by damaging associated transmission lines or control centers that may be located on site.

Because HV transformers are so big and are connected to the largest overhead transmission towers, they are easily identified along major transmission corridors. High voltage transformers are usually housed in substations that are enclosed with a chain-link fence. Guards are not often stationed at these facilities under normal operating circumstances. Consequently, HV transformers are ordinarily easier to access than other critical electric facilities such as generation plants and control centers. Utilities use closed-circuit surveillance and other methods to detect intrusion. However, access to the substation may be achieved by either cutting or scaling the chain-link fence. Once inside, a saboteur could cause damage by accessing the control room or physically damaging the HV transformer. Penetrating the 5/8 to 3/4-inch steel tank with any device could short-circuit the windings and irreparably destroy the transformer. Alternatively, a saboteur could attempt to open a valve and drain the insulating oil. Igniting the oil might cause the transformer to arc and eventually explode. With a clear line of sight, an attacker could also disable transformers from a distance using conventional rifles. Other methods of disabling HV transformers have also been identified.

The vulnerability of individual transformer substations has been demonstrated by successful attacks in recent years. In the most serious case, a rifle attack occurred in April 2013 at PG&E's 500 kV substation in Metcalf, CA. In this attack, multiple individuals outside the substation reportedly shot at the HV transformer radiators with .30 caliber rounds, causing them to leak

Nonpublic Information at the Federal Energy Regulatory Commission, DOE/IG-0933, January 2015, p. 5.

[24] Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," *Wall Street Journal*, February 5, 2014.

[25] U.S. Department of Energy, *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, April 2015, p. S-11.

[26] Mitsubishi Electric Power Products, Inc., personal communication, Warrendale, PA, September 23, 2003.

[27] Lower Colorado River Authority, "August 6 Update on Transformer Fire," press release, August 6, 2003.

cooling oil, overheat, and become inoperative.[28] In October 2013, the U.S. Justice Department charged an individual with attacks on the transmission grid in Arkansas, including a deliberate fire at Entergy's 500 kV substation in Lonoke County. The fire consumed the substation control house but electrical service was not interrupted.[29] In 2005, at a Progress Energy substation in Florida, a rifle attack ruptured a transformer oil tank, ultimately causing an explosion and local blackout.[30] Other incidents at substations have been reported with some regularity, although most have been attributed to vandals or careless hunters.

It is very difficult to restore a damaged HV transformer substation. As noted above, transmission experts assert that most HV transformers currently in service are custom designed and, therefore, cannot be generally interchanged. Furthermore, at $3-5 million per unit or more, maintaining large inventories of spare HV transformers solely as emergency replacements is prohibitively costly, so limited extras are on hand. The number of spares a utility maintains is increasingly sensitive information, but one regional transmission control area reported in 2007 that it maintained 29 spares for 188 transformers rated 500 kV on its system.[31] Programs for the sharing of spare HV transformers among multiple utilities are discussed later in this report.

Within the United States, transportation of HV transformers is difficult. Due to their size and weight, most HV transformers are transported on special railcars, each with up to 36 axles to distribute the load. There are fewer than 20 of these railcars in the Unites States rated to carry 500 tons or more, which can present a logistical problem if they are needed in a transformer emergency.[32] In some cases involving older transformers, adjacent rail lines are no longer in service, so replacement transformers may need to be transported by other means. Specialized flatbed trucks can also carry heavy transformer loads over public roadways, but the few such trucks that exist have less carrying capacity and greater route restrictions than the railcars because HV transformers may exceed highway weight limits. Transporting HV transformers, especially in an emergency, can create other logistical challenges as well, including the coordination of movement through ports and road constraints (e.g., tunnels and overpasses), special transportation permits, and police escort requirements.[33]

Targeting of HV Transformers

Malicious individuals could, without significant training, identify critical HV transformer locations and time an attack for greatest effect. This could be accomplished with basic knowledge of transmission operations and regional network characteristics drawn from publicly available sources, including electric marketing data indicating constrained areas of the network.[34] In 2014, a security services company published a summary of this kind of exercise, identifying 14 of the

[28] RTO Insider, "Substation Saboteurs 'No Amateurs'," April 2, 2014, http://www.rtoinsider.com/pjm-grid2020-1113-03/.

[29] Chelsea J. Carter, "Arkansas Man Charged in Connection with Power Grid Sabotage," CNN, October 12, 2013; Max Brantley, "FBI Reports Three Attacks on Power Grid in Lonoke County," *Arkansas Times*, October 7, 2013.

[30] Jim Peppard, "Reward Offered in Power Transformer Shooting," WTSP News (Tampa), October 17, 2005.

[31] David Egan and Kenneth Seiler, PJM Interconnection, "PJM Manages Aging Transformer Fleet," *T&D World*, March 1, 2007.

[32] Tom Daspit, "Schnabel Cars in Service," web page, August 15, 2013, http://southern.railfan.net/schnabel/schnabel_cars.html.

[33] U.S. Department of Energy, April 2015, p. S-20.

[34] Marija Ilic, Professor, Engineering and Public Policy and Electrical and Computer Engineering, Carnegie Mellon Univ., Pittsburgh, PA, personal communication, September 22, 2003.

"most critical" transformer substations in the United States based on the company's criteria.[35] As stated in a 2012 National Research Council report, "terrorists could selectively target key equipment, especially large transformers."[36] The OTA report describes such a scenario:

> [One] example is a city served by eight transmission substations spread along a 250-mile line and located in five States. A knowledgeable saboteur would be needed to identify and find the eight transmission substations. A highly organized attack would also be required. However the damage would be enormous, blacking out a four-State region, with severe degradation of both reliability and economy for months.[37]

In 1997, the Irish Republican Army reportedly planned this kind of coordinated attack against six transmission substations in the United Kingdom. Although the attack was prevented, had it been successful it reportedly could have caused widespread power outages in London and the South East of England for months.[38]

It is relatively easy to learn about HV transformer vulnerabilities from engineers and operators experienced with this technology, either domestically or abroad, since the same technology is used in power grids throughout the world. In the past, transformer experts have provided CRS with detailed descriptions of numerous "simple" ways terrorists could destroy HV transformers. General transformer sabotage information is also available on the Internet. One sabotage manual associated with white supremacist groups available online includes the following discussion:

> The power generation and distribution systems of most major Western cities are surprisingly vulnerable.... Attacking during peak consumption times (Winter in cold climates and Summer in hot climates) will make power diversion impossible.... Arson, explosives or long-range rifle fire can be used to disable substations, transformers and suspension pylons. A simultaneous attack against a number of these targets can shut down power ... with the advantage that service cannot be quickly restored by diverting power from another source. Each broken link in the power grid must be repaired in order to fully restore service. An individual, equipped with a silenced rifle or pistol, could easily destroy dozens of power transformers in a very short period of time.[39]

Security analysts and other industry officials acknowledge that the vulnerability of HV transformers in general is widely known, although understanding the criticality of particular assets within the power grid would require more dedicated effort.

Physical Security Measures for HV Transformers

Although HV transformers are relatively large and often exposed, frequently in rural areas, there are a number of measures available to help prevent an intentional physical attack against a transformer substation. Many of these measures are employed for public safety and to protect against theft, so they may serve multiple purposes. Although security measures appropriate for a particular substation vary depending upon its particular configuration and operating profile, such measures fall into a set of general categories:

---

[35] Critical Intelligence, Inc., "Grid Strike," summary report, Idaho Falls, ID, 2014. The methodology and results of this study were not independently validated; the analysis is proprietary.

[36] NRC, 2012, p.79.

[37] OTA, June 1990, pg. 37.

[38] Stewart Tendler, "IRA Bombers Plotted to Black Out London and South East for Months," *The Times*, London, England, April 12, 1997.

[39] Axl Hess (a.k.a. Aquilifer), *White Resistance Manual V2.4*, 2001. See also Herschel Smith, "A Terrorist Attack That America Cannot Absorb," captainsjournal.com, blog, September 28, 2010, http://www.captainsjournal.com/2010/09/28/a-terrorist-attack-that-america-cannot-absorb/.

- **Protecting information** about critical HV substations, such as engineering drawings, power flow modeling runs, and site security information, which could be useful to a potential attacker.
- **Surveillance and monitoring** through the use of video cameras, motion detectors, imaging, acoustical monitors, aerial drones, and periodic inspection by security employees.
- **Restricting physical access,** such as limiting entry only to necessary employees, installing electronic locks and other access controls, and erecting physical barriers and controls for vehicle entry. Posting full-time guards may also be an option in some circumstances.
- **Shielding assets** from offsite attacks using visual barriers such as opaque or hardened fencing, erecting taller fences, or erecting protective walls.
- **Modifying substation designs** to make them more resistant to physical damage, for example, by strengthening transformer cooling systems or bushings. Reconfiguring substation layouts to limit asset visibility or limit the spread of fire may also be options.

Industry and federal efforts to promote the deployment of such physical security measures are discussed later in this report. In addition to these categories, other measures can help to mitigate the immediate effects of a successful attack ("resiliency"), or to speed full system recovery from such an attack. Measures to enhance the cybersecurity of substation information and control systems, especially supervisory control and data acquisition (SCADA) systems are an important component of power grid security and are usually coordinated with physical security measures.

Sector Initiatives for HV Transformer Security

Over the last decade or so the electric utility industry and government agencies have engaged in a number of initiatives to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These initiatives include coordination and information sharing, spare equipment programs, security standards, grid security exercises, and other measures discussed below.

Coordination and Information Sharing

The *National Infrastructure Protection Plan* (NIPP), initially published by the Department of Homeland Security in 2006, "outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes."[40] The plan organizes critical infrastructure into distinct sectors, designating a federal department or agency as the lead coordinator for each sector—the Sector Specific Agency (SSA). Under the NIPP and Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, the Department of Energy (DOE) is designated as the SSA for the Energy Sector, which includes the electric utility industry (excluding nuclear power plants). As an SSA, the department is responsible for working with the Department of Homeland Security (DHS), other federal agencies, critical infrastructure owners, independent regulators, and other

[40] Department of Homeland Security (DHS), "National Infrastructure Protection Plan," web page, April 7, 2014, https://www.dhs.gov/national-infrastructure-protection-plan. The NIPP was mandated under Homeland Security Presidential Directive 7 issued on December 17, 2003.

agencies to implement national policy on critical infrastructure security and resilience.[41] The NIPP also established a sector partnership model including private and government coordinating councils:

- The **Electricity Subsector Coordinating Council (ESCC),** initially established in 2004, was organized and administered by companies in the electric power industry. It meets regularly to coordinate policy-related activities designed to "improve the reliability and resilience of the electricity subsector, including physical and cyber infrastructure."[42] Through August 15, 2013, the ESCC was chaired by the North American Electric Reliability Corporation (NERC), the not-for-profit organization responsible for ensuring the reliability of the North American grid.[43] The ESCC has since transitioned to a new structure led by electric utility industry executives, although NERC's chief executive officer remains on the ESCC steering committee.[44]
- The **Energy Sector Government Coordinating Council (EGCC),** also established in 2004, is the government counterpart to the ESCC. The EGCC is chaired by the DOE and DHS, incorporating other agencies at all levels of government with interest in energy security. The EGCC plays a key role in implementing the Sector-Specific Plan (discussed below), collaborating with the ESCC to develop and prioritize security programs and initiatives.[45]

In addition to these councils, other organizations have been established with more specific responsibilities related to grid security.

- The **Electricity Sector Information Sharing and Analysis Center (ES-ISAC),** established in 1998, is the electricity sector's primary communications channel for security-related information, situational awareness, incident management, and coordination.[46] The ES-ISAC is operated by NERC in collaboration with the DOE and ESCC. Members may anonymously share security-related incident information with the ES-ISAC by means of a secure Internet portal. Registered users receive information on security threats and alerts, remediation, task forces, events, and other security-specific resources.[47]
- NERC's **Critical Infrastructure Protection Committee (CIPC)** coordinates NERC's security initiatives and advises NERC's Board of Trustees, its standing physical and cybersecurity committees, and the ES-ISAC. One of the CIPC's key

[41] Presidential Policy Directive 21, *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, February 12, 2013.

[42] North American Electric Reliability Corporation (NERC), "Electricity Sub-sector Coordinating Council," web page, April 7, 2014, http://www.nerc.com/pa/CI/Pages/ESCC.aspx.

[43] Among other functions, NERC develops and enforces reliability standards, monitors the grid, and trains industry personnel. In the United States, NERC is subject to Federal Energy Regulatory Commission oversight.

[44] Gerry W. Cauley, North American Electric Reliability Corporation (NERC), letter to U.S. Secretary of Energy Ernest Moniz, August 23, 2013, http://www.publicpower.org/files/PDFs/DOESecLetterHistoryESCC.pdf.

[45] Department of Energy, *Energy Sector-Specific Plan*, 2010, p. 20.

[46] The ES-ISAC was established under Presidential Decision Directive 63, May 22, 1998.

[47] Electricity Sector Information Sharing and Analysis Center (ES-ISAC), "Frequently Asked Questions," web page, https://www.esisac.com/SitePages/FAQ.aspx.

functions is developing, reviewing, and revising security guidelines; and assisting in the development and implementation of NERC standards.[48]

- In January 2015, NERC chartered the **Physical Security Advisory Group (PSAG)**—consisting of representatives from the electric power industry, DOE, DHS, and informed observers—to assist the ES-ISAC in the analysis of physical security threats. The PSAG is intended to offer advice on security plans, policy and procedure, security technology, training, incident response, and threat mitigation strategy to enhance grid physical security and reliability.[49]

DOE's Energy Sector-Specific Plan

The 2006 *National Infrastructure Protection Plan* required each critical infrastructure sector to develop a Sector-Specific Plan (SSP) that describes strategies to protect its critical infrastructure, outlines a coordinated approach to strengthen its security efforts, and determines appropriate funding for these activities. The section of the DOE's *Energy Sector-Specific Plan* addressing electricity was developed in collaboration with the ESCC and EGCC. The plan identifies high-voltage transformers as an electric sector vulnerability due to their criticality to the power grid and the difficulty of replacing them in the event of a successful attack. Among other measures, the SSP established a goal of implementing "agreements that require participants to maintain transformers for possible sharing in the event of a terrorist act."[50] The plan also identified the "need for a new type of emergency spare (recovery/mobile) high-voltage transformer that can be deployed and energized quickly to rapidly recover from outages caused by natural disasters and deliberate attacks."[51]

ESCC's Critical Infrastructure Strategic Roadmap

In November 2010, the Electricity Subsector Coordinating Council published its *Critical Infrastructure Strategic Roadmap* report, to provide a framework for identifying risks that could seriously disrupt the grid and for promoting actions to enhance grid reliability and resilience. The report paid particular attention to "severe-impact risks with the potential to impact large portions of the grid, or disrupt service for an extended period of time."[52] The report considered three principal risk scenarios, the first of which relates to physical attacks:

> **Scenario 1: Physical Attack on Significant Electricity System Equipment**
> A coordinated physical attack on key nodes of the bulk power system critically disables difficult to replace equipment in multiple generating stations or substations and could have a significant affect [sic] on the remainder of the system. A prolonged period of time is required to fully restore the bulk power system to normal operation.[53]

[48] North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection Committee (CIPC)," web page, http://www.nerc.com/comm/CIPC/Pages/default.aspx, April 8, 2014.

[49] North American Electric Reliability Corporation, "ES-ISAC Physical Security Advisory Group (PSAG) Charter," January 20, 2015.

[50] Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 54.

[51] Department of Homeland Security, *Energy Sector-Specific Plan*, 2010, p. 70.

[52] North American Electric Reliability Corporation (NERC), *Critical Infrastructure Strategic Roadmap*, November 2010, p. 2, http://ccpic.mai.gov.ro/docs/NERC_ESCC_Critical_Infrastructure_Strategic_Roadmap.pdf.

[53] NERC, November 2010, p.18. This scenario involved the loss of three HV substations serving large urban centers with a restoration time to 100% operating capacity of 6-18 months.

The report recommended an assessment of current capability to prevent and respond to such a scenario as a "high priority." The report also recommended as "important" both a study of "options and practices to enhance physical protection of critical equipment requiring long recovery times (e.g., large high-voltage transformers)" and an initiative to "enhance the availability of critical spare equipment ... starting with high voltage transformers."[54]

EEI's Threat Scenario Project

In 2011, the Edison Electric Institute (EEI), the main trade association for U.S. investor-owned electric utilities, initiated its Threat Scenario Project to identify security threats and practices utilities could take to mitigate these threats. While the project examined a wide range of potential threats, it included consideration of coordinated physical and cyberattacks.[55] According to EEI, "the project established common elements for each threat scenario, including a description, likely targets, potential threat actors, specific attack paths, and likely impacts of a successful attack."[56] The project is ongoing, with the goal of helping electric utilities "quickly identify areas where security measures are sufficient and where gaps may exist, and begin the dialogue about additional measures that can be taken to help detect, protect against, respond to, and recover from a range of potential threat scenarios."[57]

DOE's Quadrennial Energy Review

As stated above, in April 2015, the DOE released its first *Quadrennial Energy Review* (QER), focusing on energy infrastructure, including "resilience, reliability, safety, and asset security for the electric grid."[58] Among its considerations related to the electric grid, the report focuses specifically on the security of HV transformers.

> The Administration has made it a priority to work with industry to identify challenges and create solutions for increasing the security and resilience of the electric grid, including the development of an integrated national plan to mitigate challenges pertaining to aging power transformers, the cyber and physical security of transformers, and the vulnerabilities of large power transformers. The Administration is working with trade association leadership and the private sector to improve the coordination of existing and planned transformer-sharing programs and to identify solutions for transformer replacement capabilities as part of its efforts to enhance the resilience of the Nation's electric grid.[59]

The QER also specifically recommended that DOE should lead a multi-agency (federal and state) and industry initiative to mitigate the risks of HV transformer losses, including the development of additional transformer reserves as discussed below.[60]

---

[54] NERC, November 2010, pp.19-20.

[55] Edison Electric Institute and Chertoff Group, "EEI Business Continuity Conference Threat Scenario Project (TSP)," slide presentation, April 4, 2012, http://www.eei.org/meetings/Meeting_Documents/2012Apr-BusinessContinuity-Treat%20Scenario%20Project_Engels.pdf.

[56] Edison Electric Institute, "Electric Power Industry Initiatives to Protect the Nation's Grid From Cyber Threats," fact sheet, January 2013, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity%20Industry%20Initiatives.pdf.

[57] Chertoff Group, "Addressing Dynamic Threats to the Electric Power Grid through Resilience," November 2014, p. 5.

[58] U.S. Department of Energy, April 2015, p. 2-8.

[59] U.S. Department of Energy, April 2015, p. 2-15.

[60] U.S. Department of Energy, April 2015, p. 2-40.

Transformer Equipment Programs

Consistent with the recommendations of the studies above, several programs have been instituted within the electric power sector to address the operational issues that could emerge due to the scarcity of spare HV transformers and associated equipment in the event of a physical attack or other grid emergency.

DHS Recovery Transformer Program

In 2008, the Department of Homeland Security (DHS) initiated a program to develop a prototype "Recovery Transformer" (RecX) which could enable recovery from transformer failure within days rather than months or longer.[61] The RecX transformer was intended to be adaptable to a range of common grid specifications as well as being smaller, lighter, easier to transport, and quicker to install than conventional HV transformers. The RecX prototype was designed to replace the most common HV transformers (345 kV) used in the U.S. grid.[62] This design reportedly could be used to replace approximately one quarter of the 2,100 transformers in this voltage class currently deployed.[63] In 2012, the only three single-phase RecX prototype units were installed in an operating 345 kV substation in Texas during a simulated emergency drill, where they remain in regular operation, having met or exceeded their service requirements.[64] The RecX transformers have reliability and efficiency characteristics comparable to other 345 kV transformers, and are also comparably priced ($7.5 million each).[65] Although the manufacturer has received no orders for commercial production of these units as of May 2015, a few utilities have expressed interest in leveraging the concepts demonstrated by the RecX program for their own applications.[66] Having successfully demonstrated the RecX concept, the DHS is no longer funding the RecX program, but the manufacturer has discussed continued development of the concept including higher kV ratings and "hardened" designs.[67]

EEI Spare Transformer Equipment Program

In 2006, the Edison Electric Institute initiated its Spare Transformer Equipment Program (STEP) to strengthen "the sector's ability to restore the nation's transmission system more quickly in the event of a terrorist attack."[68] The STEP program requires participating utilities to maintain (or acquire) a specific number of transformers up to 500 kV to be made available to other utilities in case of a critical substation failure. Sharing of transformers is mandatory based on a binding contract subject to a "triggering event"—a coordinated act of deliberate, documented terrorism resulting in the destruction or disabling of a transmission substation and the declaration of a state

[61] The program was partly funded by the DHS Science and Technology Directorate in a consortium with the Electric Power Research Institute, CenterPoint Energy, and ABB.

[62] ABB, "US Rapid Recovery Transformer Initiative Succeeds Using Specially-Designed ABB Transformers," press release, October 4, 2012.

[63] Matthew L. Wald, "A Drill to Replace Crucial Transformers (Not the Hollywood Kind)," *New York Times*, March 14, 2012.

[64] EPRI, September 30, 2014, p. 7.

[65] National Research Council (NRC), *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*, 2013.

[66] Sarah Mahmood, Department of Homeland Security, personal communication, May 28, 2015.

[67] ABB, "ABB and U.S. Policymakers Meet to Address Grid Vulnerability Issues," press release, May 21, 2015.

[68] Edison Electric Institute (EEI), "Spare Transformers," web page, April 10, 2014, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx.

of emergency by the President.[69] FERC granted blanket authorization for the transfer and cost recovery of transmission equipment under the STEP program in September 2006.[70] State regulators with jurisdiction over participating utilities have also granted pre-approval for STEP transfers.[71] The program is designed to deal with terrorist events, but it also provides a mechanism for voluntary sharing of transformers in other emergencies, although these may require additional regulatory approvals. EEI requires annual recertification and conducts a STEP program drill every summer to ensure the program and its members will be fully prepared to respond in the event of an actual triggering event.[72]

NERC Spare Equipment Database

In 2012, NERC initiated its Spare Equipment Database (SED) program intended to serve as a tool to "facilitate timely communications between those needing long-lead time equipment damaged in a [high impact, low frequency] event and those equipment owners who may be able to share existing equipment being held as spares by their organization."[73] The SED program is a confidential web-based catalog of spare transformers rated at 100 kV or higher. Only NERC and the equipment owners can see their spares data (although NERC can make high-level reports to FERC); requests for equipment disclose neither the requester nor provider (double-blind). Participation is voluntary and requires no commitment or mandatory sharing of spares.[74] Unlike EEI's STEP program, however, the SED program has not been granted pre-approval from FERC or state regulators for equipment transfers. Thus, the ability to transfer the ownership of transformers from one company to another may require additional approvals, even during an emergency.

QER Transformer Reserve Proposal

The DOE's *Quadrennial Energy Review* states that the inventory of HV transformers under EEI's STEP program is too small to respond to a large, coordinated attack against critical substations, and that transformer design variations and logistics further limit the effectiveness of EEI's program.[75] Accordingly, the QER recommends a DOE-led effort to develop one or more HV transformer reserves through a staged process involving: assessment of technical specifications for reserve transformers, where to locate transformers, how many would be needed, how they would be secured and maintained, how they might be transported, and whether new federal authorities or cost sharing would be necessary.[76] Consistent with this recommendation, a House bill to establish a Strategic Transformer Reserve program (H.R. 2244) introduced on May 8, 2015, would require the Secretary of Energy to submit to Congress "a plan to establish a Strategic

[69] Edison Electric Institute (EEI), "Overview of the Spare Transformer Equipment Program," slide presentation, February 23, 2014.

[70] Federal Energy Regulatory Commission, *Order on Application for Blanket Authorization for Transfers of Jurisdictional Facilities and Petition for Declaratory Order*, Docket Nos. EC06-14-000 and EL06-86-000, September 22, 2006.

[71] EEI, February 23, 2014.

[72] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

[73] North American Electric Reliability Corporation (NERC), *Special Report: Spare Equipment Database System*, August 2011.

[74] North American Electric Reliability Corporation (NERC), "Spare Equipment Database," slide presentation, NERC Industry Webinar, July 22, 2013, http://www.nerc.com/pa/RAPA/webinardl/SED_Presentation_July_22_2013.pdf.

[75] U.S. Department of Energy, April 2015, p. 2-11.

[76] U.S. Department of Energy, April 2015, p. 2-40.

Transformer Reserve for the storage, in strategically located facilities, of spare large power transformers in sufficient numbers to temporarily replace critically damaged large power transformers" (Sec. 1(c)(1)). Implementation and funding of such a plan would be subject to congressional approval.

Grid Assurance LLC

On June 10, 2015, a group of eight electric utilities and energy companies[77] announced a new private sector joint venture company called Grid Assurance "to provide improved responses to major events affecting the electric transmission grid by giving transmission-owning entities access to domestically warehoused long lead-time critical equipment," including HV transformers.[78] Grid Assurance would function as a service company open to other transmission companies via a standardized subscriber agreement. Subscription would be voluntary. In an associated filing with FERC, Grid Assurance states that it will

> (1) maintain an optimized inventory of critical spare transformers, circuit breakers and related transmission equipment,
>
> (2) provide secure domestic warehousing of the inventory of spares in strategic locations, and
>
> (3) release spare equipment to utility subscribers as needed to respond to emergencies.[79]

The company believes its services will be complementary to, but significantly broader than, EEI's Spare Transformer Equipment Program. It will offer transformers in a wider range of voltage classes, other long-lead time equipment (e.g., circuit breakers, phase angle regulators, temporary towers), and greater logistical support, among other services.[80] Grid Assurance has petitioned FERC for a declaratory order affirming that contracting with the company would be permissible as part of a physical security plan under NERC physical security regulations (discussed below), and that acquisition of equipment by utility subscribers from Grid Assurance would not require authorization under Section 203 of the Federal Power Act.[81]

Grid Security Exercises and Simulations

NERC and FERC have conducted grid security computer simulations and exercises specifically incorporating hypothetical attacks on HV transformer substations.

GridEx and GridEx II

In 2011, NERC conducted GridEx 2011, its first electric sector-wide grid security exercise. The exercise assessed the readiness of utilities to respond to a cyberattack, strengthened their crisis response, and provided input for internal security program improvements. Although the exercise was focused on a cyberattack, it did involve physical incursions into power grid substations as

[77] American Electric Power (AEP), Berkshire Hathaway Energy, Duke Energy, Edison International, Eversource Energy, Exelon, Great Plains Energy, and Southern Company.

[78] Grid Assurance, LLC, "Eight Utilities and Energy Companies Announce Plans for Critical Transmission Equipment Service Company," press release, June 10, 2015, http://gridassurance.com/lib/docs/Grid%20Assurance%20New%20Release%20FINAL%206-9.pdf.

[79] Grid Assurance LLC, Petition for Declaratory Order and Request for Expedited Action filed with the Federal Energy Regulatory Commission, Docket No. EL15-, June 9, 2015, p. 1.

[80] Grid Assurance, LLC, June 9, 2015, pp. 20-21.

[81] Grid Assurance, LLC, June 9, 2015, pp. 22-23.

well as aspects of grid monitoring and recovery that would be relevant to an attack on HV transformers.[82] Among other findings, the exercise determined that "utilities took appropriate steps to secure the grid."[83] Nonetheless, NERC recommended that "entities should ensure their response protocols address a coordinated threat," and that it would "facilitate and support the development of updated physical security guidance."[84]

After the Metcalf attack in 2013, NERC conducted a second, more expansive grid security exercise, GridEx II. The exercise scenario, developed using open-source techniques, included a cyberattack on the grid coupled with a coordinated physical attack against a subset of transmission and generation assets—including HV transformer substations.[85] Among other conclusions, NERC's after-action report stated:

> While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.... The extreme challenges posed by the Severe Event scenario provided an opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.[86]

NERC did not publicly report details about the overall impacts to the grid or outages in particular regions due to the sensitive nature of such information. Utilities and other agencies participating in the exercise viewed it a useful tool for utilities to test their readiness and preparedness for attacks on the grid.[87] NERC is in the process of preparing for GridExIII to be conducted in November 2015.

FERC "Electrically Significant Locations" Study

In early 2013, prior to the Metcalf attack, then-FERC Chairman John Wellinghoff directed FERC staff to prepare an analysis identifying critical HV substations in the North American power grid.[88] Using power flow analysis software to model the impacts to the transmission system from the loss of specific grid assets,[89] FERC staff compiled a list of "Electrically Significant Locations (ESLs)" within the grid.[90] Neither details of the ESL study methodology nor its results have been

[82] North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. i.

[83] NERC, 2012, p. ii.

[84] Ibid.

[85] North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.15; Matthew L. Wald, "Attack Ravages Power Grid. (Just a Test.)," *New York Times*, November 14, 2013.

[86] NERC, March 2014, p. 5.

[87] See, for example, American Public Power Association, "Physical Security and the Electric Sector," fact sheet, February 2014, http://www.publicpower.org/files/PDFs/PhysicalSecurityIBFebruary2014.pdf; Matthew L. Wald, "Power Grid Preparedness Falls Short, Report Says," *New York Times*, March 12, 2014.

[88] Federal Energy Regulatory Commission (FERC), "Second Set of Responses of the Federal Energy Regulatory Commission to Senator Murkowski's Separately Submitted Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee," May 5, 2014, pp. 12-13, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5c3bf9d7-bb7f-4379-8f57-f58881a0b5d6.

[89] FERC staff employed the commission's Topological and Impedance Element Ranking (TIER) model to identify "significant" assets based upon undisclosed criteria. For more details of the TIER model, see Bernard C. Lesieutre et al., "Topological and Impedance Element Ranking (TIER) of the Bulk-Power System," University of Wisconsin—Madison, prepared for the Federal Energy Regulatory Commission, August 2009, https://www.ferc.gov/EventCalendar/Files/20090911112656-TIER%20REPORT.pdf.

[90] Federal Energy Regulatory Commission (FERC), "Response to Senator Murkowski's Separately Submitted

released publicly by FERC or other agencies, although some findings have been reported in the press and discussed publicly by federal officials. According to the *Wall Street Journal*, the FERC analysis identified 30 critical transformer substations; in FERC's simulation, losing nine of these substations (in various combinations) as the result of a coordinated attack reportedly was found to cause a nationwide blackout for an extended time.[91] As noted above, however, DOE officials have questioned the validity of FERC's analysis.

Members of Congress were highly critical of both the *Wall Street Journal* and FERC officials for inappropriately releasing what was perceived to be highly sensitive information about power grid physical vulnerability.[92] The study was not initially designated as security sensitive by commission staff. A subsequent investigation by the Department of Energy's Inspector General concluded that FERC's handling of the ESL study findings was improper.[93] The protection of information about grid security is further discussed in a later section of this report.

HV Transformer Security Standards

Several grid security guidelines or standards have been developed or proposed to address the physical security of the grid, including HV transformers. These standards have been promulgated by NERC as voluntary best practices since at least 2002, with subsequent revisions. However, in the wake of the Metcalf incident, FERC ordered the imposition of mandatory physical security standards in 2014. Current industry-wide standards are discussed in the following sections.

IEEE Substation Security Standard

In 2000, the Institute of Electrical and Electronics Engineers (IEEE), a technical professional society, published its first standards for electric power substation physical and electronic security. The voluntary standard addressed "security issues related to human intrusion upon electric power supply substations" and various methods to mitigate them.[94] The original standard, and subsequent revisions, call for the development of security assessments and, for "high-risk areas," increased security measures such as motion detectors, perimeter/area detection systems, security cameras, physical barriers, and posted guards.[95] However, according to the IEEE, the standard is intended to address security issues related to unauthorized access, theft, and vandalism. The IEEE states that "attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc. are beyond the scope of this standard."[96]

Questions for the Record from April 10, 2014 Hearing of the Senate Energy and Natural Resources Committee, Question 39," May 5, 2014, p. 2, http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=2826f80a-a986-45d1-9261-87b45e1d6872.

[91] Rebecca Smith, "U.S. Risks National Blackout from Small-Scale Attack on Substations," *Wall Street Journal*, March 13, 2014.

[92] Senate Committee on Energy and Natural Resources, "Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities," press release, March 31, 2014.

[93] U.S. Department of Energy, Office of Inspector General, "Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission," DOE/IG-0906, April 9, 2014.

[94] Institute of Electrical and Electronics Engineers (IEEE), *1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security*, January 30, 2000.

[95] IEEE, January 30, 2000, p. 16.

[96] Institute of Electrical and Electronics Engineers (IEEE), "P1402—Standard for Physical Security of Electric Power Substations," web page, June 3, 2015, http://standards.ieee.org/develop/project/1402.html.

NERC Physical Security Guidance

In June 2002, NERC published its initial guidance for physical response to security alerts from the federal government. This alert system was revised in October 2002 to correspond to DHS's new color-coded threat level system.[97] NERC's guidance was voluntary, intended to provide "examples of security measures that electric utility organizations may consider taking, based on the Alerts issued."[98] NERC's guidance included 35 specific security measures for the five threat DHS levels. These measures ranged from "occasional" workforce awareness programs and annual security plan reviews during times of low threat (green) to continuous monitoring of critical facilities, potentially with armed guards, during times of highest threat (red).[99] Along with this guidance, NERC published initial guidelines for vulnerability and risk assessment to help identify critical facilities and countermeasures to mitigate threats.[100]

In November 2005, NERC published a third version of its physical security guidelines, to provide "examples of security measures that other electricity sector organizations *should* consider when responding to threat level alerts" [emphasis added].[101] Thus, while still voluntary, these measures appear to have been intended as recommendations rather than considerations as stated in the earlier versions. The 2005 document included 55 measures, including new measures and existing measures expanded or described more specifically. New measures during times of low threat included, for example, annual audits of critical facility access programs and identifying critical facility long-term and short-term security measures (e.g., vulnerability assessments and security barriers).[102]

The Energy Policy Act of 2005 (P.L. 109-58) mandated the implementation of electric grid reliability standards under new authority granted to the Federal Energy Regulatory Commission. FERC subsequently designated NERC as the Electric Reliability Organization certified by the commission to establish and enforce reliability standards for the U.S. electric transmission grid, subject to commission review. In 2008, FERC approved NERC's initial reliability standards for critical infrastructure; however, these standards were developed primarily to address transmission grid cybersecurity, not physical security.[103] Subsequent NERC standards have expanded these cybersecurity requirements.

In October 2013, NERC published its most recent revision to its physical security guidance, *Security Guideline for the Electricity Sub-sector: Physical Security Response,* providing to electricity sector members "actions they should consider when responding to the threat alerts" issued by the DHS.[104] Continuing its voluntary (rather than regulatory) approach to physical

---

[97] North American Electric Reliability Corporation (NERC), *Threat Alert System and Physical Response Guidelines for the Electricity Sub-sector*, Version 2.0, October 8, 2002, http://www.iwar.org.uk/infocon/threat-levels/tas_physical_V2.pdf.

[98] NERC, October 8, 2002, p. 2.

[99] NERC, October 8, 2002, pp. 3-4.

[100] NERC, *Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment*, June 14, 2002, http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Vulnerability%20and%20Risk%20Assessment,%20Version%201.0.pdf.

[101] NERC, *Security Guidelines for the Electricity Sector: Physical Response*, November 1, 2005, p.1, http://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Physical%20Response,%20Version%203.0.pdf.

[102] NERC, November 1, 2005, p. 3.

[103] FERC Order 706.

[104] North American Electric Reliability Corporation (NERC), *NERC: Security Guideline for the Electricity Sub-sector: Physical Security Response*, October 28, 2013, p. 1, http://www.nerc.com/comm/CIPC/SecurityGuidelinesCurrent/

security, NERC's guidance states that "each organization decides the risk it can accept and the practices it deems appropriate to manage its risk."[105] This version of NERC's guidance lays out 77 distinct security measures corresponding to three levels of threat: (1) Normal Operations/Best Practices, (2) Elevated, and (3) Imminent.

FERC Physical Security Best Practices

In 2013, FERC staff along with staff from the Federal Bureau of Investigation (FBI), DOE, DHS, and NERC participated in a number of meetings with utilities and law enforcement agencies to discuss immediate findings and recommendations stemming from the Metcalf substation attack. As part of these meetings, FERC staff shared with utilities a list of best practices for physical security. Although the list has not been made public, it reportedly included prescriptive security measures (e.g., outward-facing video surveillance) focused on security threats similar to that experienced at the Metcalf substation.[106] In 2014, DHS, in coordination with FERC, the ES-ISAC, NERC, the FBI, and industry experts, convened another series of regional briefings across North America with utilities and law enforcement officials to follow up on the initial outreach regarding substation physical security.[107]

NERC Physical Security Regulations

On March 7, 2014, FERC ordered NERC to submit to the commission within 90 days proposed reliability standards requiring certain transmission owners "to take steps or demonstrate that they have taken steps to address physical security risks and vulnerabilities related to the reliable operation" of the power grid.[108] In its order FERC stated that physical security standards were necessary because "the current Reliability Standards do not specifically require entities to take steps to reasonably protect against physical security attacks."[109] According to FERC's order, the new reliability standards were to require transmission owners or operators to perform a risk assessment of their systems to identify their "critical facilities," evaluate the potential threats and vulnerabilities to those identified facilities, and develop and implement a security plan designed to protect against attacks to those identified critical facilities.[110] The order required that each of these steps be verified by NERC or another third party qualified to review them.

On May 23, 2014, NERC filed with FERC its proposal for mandatory physical security standards.[111] On November 20, 2014, FERC approved the proposed standard, with minor

Electricity%20Sector%20Physical%20Security%20Guideline%20(Approved%20by%20CIPC%20-%20October%2028,%202013).pdf.

[105] NERC, October 28, 2013, p.1.

[106] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

[107] Gerry Cauley, CEO, North American Electric Reliability Corporation (NERC), letter to Senator Harry Reid, February 12, 2014, p. 2, http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf.

[108] Federal Energy Regulatory Commission (FERC), *Reliability Standards for Physical Security Measures*, Order Directing Filing of Standards, Docket No. RD14-6-000, March 7, 2014, p.1, http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf.

[109] FERC, March 7, 2014, p. 2.

[110] FERC, March 7, 2014, pp. 3-4.

[111] North American Electric Reliability Corporation (NERC), Petition of the North American Electric Reliability Corporation for Approval of Proposed Reliability Standard CIP-014-1, May 23, 2014, http://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Petition%20-%20Physical%20Security%20CIP-014-1.pdf.

changes, as NERC's new Physical Security Reliability Standard (CIP-014-1).[112] The standard applies to transmission owners with assets operating at 500 kV or higher as well as owners with substations operating between 200 kV and 499 kV if they meet certain interconnection or load-carrying criteria.[113] The standard consists of six principal requirements (R1-R6), summarized as follows:

R1. Risk assessments by transmission owners to identify critical transmission facilities;

R2. Independent third party verification of risk assessments conducted under R1;

R3. Requirement for transmission owners with critical facilities identified under R1 but not under their operational control to notify the transmission operator of these facilities;[114]

R4. Mandatory threat and vulnerability assessments for critical facilities conducted by transmission owners and operators;

R5. Development, documentation, and implementation of physical security plans to protect critical facilities; and

R6. Independent third party review of the threat and vulnerability assessments performed under R4 and security plans developed under R5.[115]

The standard also lays out a process for compliance monitoring and assessment including audits, self-certifications, spot checking, violation investigations, self-reporting, and handling complaints.[116] The new standard will be enforced by NERC or another Regional Entity under a penalty review policy for mandatory reliability standards approved by FERC subject to the Commission's enforcement authority and oversight under P.L. 109-58.[117] According to NERC, the CIP-014-1 physical security standard has staggered enforcement dates with compliance obligations beginning on October 1, 2015.[118]

Company-Specific Initiatives

Electric utilities have long had an ongoing responsibility to ensure grid reliability, in part through operating practices and investments related to grid safety and security.[119] As the standards discussed in the previous section suggest, there has been some level of physical security investment and an increasing refinement of grid security practices across the electric power sector

[112] Federal Energy Regulatory Commission, "Physical Security Reliability Standard," Docket No. RM14-15-000, Order No. 802, November 20, 2014.

[113] North American Electric Reliability Corporation (NERC), *CIP-014-1 – Physical Security*, printed June 4, 2015, p. 1, available at http://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=UnitedStates.

[114] A regional transmission operator (RTO) administers the transmission grid for multiple transmission owners in a specified region in accordance with FERC Order No. 2000. RTOs and independent system operators (ISOs) are defined in Section 3 of the Federal Power Act (16 U.S.C. 796).

[115] NERC, CIP-014-1, p. 6.

[116] NERC, CIP-014-1, p. 8.

[117] Federal Energy Regulatory Commission (FERC), *Statement of Administrative Policy on Processing Reliability Notices of Penalty and Order Revising Statement in Order No. 672*, Docket Nos. AD08-6-000 and RM05-30-002, April 17, 2008.

[118] Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, p.5.

[119] For example, see security discussion in Con Edison, "Initial Brief on Behalf of Consolidated Edison Company of New York, Inc. in Support of a Permanent Electric Rate Increase," Before the New York State Public Service Commission, November 30, 2007, http://media.corporate-ir.net/media_files/irol/61/61493/total120507.pdf.

for at least the last 15 years. Nonetheless, several major transmission owners have announced significant new investment initiatives specifically to improve the physical security of critical transformer substations in light of the Metcalf attack. Other utilities have included new substation security investments in broader initiatives for company security.[120] The following examples illustrate the types of security changes announced by these grid owners. Note that other major utilities have not publicly announced similar new security initiatives, or have kept the details of their security initiatives confidential. A comprehensive review or comparison of physical security plans among all major grid owners in the United States is beyond the scope of this report.

The Tennessee Valley Authority

In February 2012, the Tennessee Valley Authority (TVA) announced that it was "realigning its operations and structure to enhance security at TVA's non-nuclear power facilities ... focusing more of our non-nuclear security resources on our critical infrastructure," including HV substations.[121] The realignment included ending uniformed patrols in favor of installing more security technology, and the stationing of contract guards 24 hours a day at critical facilities. Together with local law enforcement cooperation, the shift to contract guards was intended to provide a more persistent security presence and faster incident response at key locations. Among the security technologies reportedly deployed by TVA are "surveillance, infrared cameras, video analytics for alarm verification and assessment, virtual perimeters, card readers, [and] automated gates."[122] TVA's security initiatives in 2012 appear to have been motivated primarily by security concerns such as copper theft, but would be applicable to more serious security risks such as terror attacks.

In February 2014, after the Metcalf incident, TVA reportedly stated that it was "intensifying efforts" to educate local law enforcement about the importance of substations, including taking police on site visits to see substations during normal operations.[123] The utility also began canvassing residents near TVA property asking them to report unusual activity around grid facilities. TVA officials have not publicly released details of the authority's physical security program, but the authority reportedly "takes significant steps, both physically and procedurally, to protect its transmission infrastructure," employing "several layers of protection."[124] TVA's *Budget Proposal and Management Agenda* for FY2016 discusses $25 million to $35 million in cybersecurity investments but does not discuss investments specifically for physical security.[125] The authority's quarterly report states that "TVA continues to evaluate measures that may be required for compliance" with FERC's new physical security standard "but costs cannot be estimated at this time."[126]

---

[120] See Southern California Edison, *Safety, Security, & Compliance (SS&C):Volume 4—Corporate Security and Business Resiliency*, 2015 General Rate Case, Before the Public Utilities Commission of the State of California, November 2013, http://www3.sce.com/sscc/law/dis/dbattach5e.nsf/0/0B9F998127246B4288257C21008148B0/$FILE/SCE-07%20Vol.%2004.pdf.

[121] Tennessee Valley Authority, "TVA Realigns Security to Enhance Protection at Non-Nuclear Assets," press release, February 17, 2012, http://www.tva.gov/news/releases/janmar12/tvap.html.

[122] "Addressing Cyber and Physical Risks in Modern Utility Security," *Security*, March 1, 2014, http://www.securitymagazine.com/articles/85275-addressing-cyber-and-physical-risks-in-modern-utility-security.

[123] Rebecca Smith, "U.S. Utilities Tighten Security After 2013 Attack," *Wall Street Journal*, February 9, 2014.

[124] Holly Meyer, "Attacks on Power Grid Point Out Vulnerabilities," *The Tennessean*, March 24, 2015.

[125] Tennessee Valley Authority, *Budget Proposal and Management Agenda*, February 2015, p. 16.

[126] Tennessee Valley Authority, Form 10-Q, April 30, 2015, p. 57.

Pacific Gas and Electric (PG&E)

In February 2014, in response to the attack on its Metcalf substation, PG&E announced that it would be investing approximately $100 million over three years to improve substation security. Physical security measures mentioned by the company included new perimeter barriers, shielding for certain equipment, more cameras (inside and outside the fence), and clearing vegetation. For its most critical facilities, the company was "studying advanced detection technology such as night vision and thermal imaging."[127] Other security measures mentioned in news reports about PG&E included enhanced lighting, 24-hour security guards, and increased patrols by local law enforcement agencies.[128] Initial implementation of these measures was inadequate, however, as the Metcalf substation experienced another significant security incident in August 2014, during which thieves breached a perimeter fence and stole several pieces of construction equipment. According to PG&E, human error was a factor because "fence detection alarms received in security operations were not appropriately addressed."[129]

Dominion

In February 2014, Dominion Virginia Power, an operating company of Dominion, announced plans to spend up to $500 million over five to seven years "to harden its transmission substations and other critical infrastructure against man-made physical threats and natural disasters, as well as stockpile crucial equipment for major damage recovery."[130] Dominion reportedly began to increase substation security efforts in 2013, focusing first on substations at greatest risk.[131] Among the security measures identified by the utility are physical barriers, additional access control, equipment design/hardening, polymer bushing installation, additional spare equipment, and relocation of spare equipment to off-site storage areas. Other measures reportedly include dual-perimeter "no man zones" around substations and installing systems for key-card access to substation yards.[132] As of February 2015, Dominion had begun implementing a series of new physical measures including new risk assessment models, modifications to substation equipment, and improved off-site monitoring.[133]

Bonneville Power Administration

In its 2014 draft *Security Asset Management Strategy*, the Bonneville Power Administration (BPA) proposed approximately $37 million in additional capital spending through FY2020 for physical security measures at approximately 60 critical transformer substations.[134] BPA's *Strategy*

[127] Geisha Williams, Executive Vice President of Electric Operations, Pacific Gas and Electric Company, "PG&E Metcalf Attack: Gunfire on Substation Has Led to Greater Security," *San Jose Mercury News*, April 15, 2014.

[128] "PG&E to Spend $87M on Security to Protect Large Substations from Attack," KTVU, Oakland, CA, February 12, 2014.

[129] Pacific Gas and Electric, "PG&E Asks for Public's Help to Support Theft Investigation at Metcalf Substation," press release, August 27, 2014.

[130] Dominion. "Substation Security," fact sheet, Spring 2014, https://www.dom.com/about/electric-transmission/pdf/substation-security-soc-factsheet.pdf.

[131] Tracy Sears, "Troopers Increase Security at Virginia Substations Critical to Grid," WTVR, March 11, 2014.

[132] Peter Bacqué, "Va. Power to Spend Up to $500M on Security Plan," *Richmond Times-Dispatch*, February 8, 2014.

[133] David Roop, Director Electric Transmission Operations, Dominion Virginia Power, "Substation Security and Resiliency—Update on Accomplishments Thus Far," slide presentation, iPCGRID 2015 Conference, March 26, 2015, https://www.cavs.msstate.edu/iPCGRID_Registration/presentations/2015/Roop_i-PCGRID_2015_Substation_Security_and_Resiliency.pdf.

[134] Bonneville Power Administration (BPA), *Security Asset Management Strategy*, February 2014, p. 29,

stated that, over the prior 13 years, the utility had "conducted hundreds of security and risk assessments using several industry accepted methodologies," and began implementing security improvements based on these risk assessments beginning in 2001.[135] The administration's 2015 "2nd Quarter Capital Project Status Report" includes $49.9 million in capital spending to acquire five 500 kV spares and relocate two existing transformers to be used as spares placed strategically across the BPA system.[136] BPA has 105 single-phase transformers (35 banks) rated at 500kV in service.[137]

New York Power Authority

The New York Power Authority (NYPA) in January 2015 requested authorization from its trustees for $42.5 million in capital expenditures primarily for physical security upgrades at critical substation in its transmission system.[138] Planned upgrades include fence intrusion detection systems, modification of physical security perimeters, installing key card access systems, surveillance cameras, laser detection systems, and associated control and monitoring systems, among other measures.[139]

Pepco Holdings

In May 2014, Pepco Holdings reportedly announced a $40 million project to upgrade physical security at various substations in the company's transmission system.[140] The company states that it has established a physical security working group, has conducted on-site physical security assessments, and has been collaborating with other entities to focus on the best security improvement opportunities. Pepco's physical security measures include guarded facilities for spare equipment, enclosing substations, improving communications connectivity, maintaining spare equipment, and considering physical security when evaluating new facilities.[141]

Issues for Congress

The recent transformer substation incidents, together with federal grid security exercises, have focused attention on the vulnerability of HV transformer substations to organized physical attacks. As the electric power industry and federal agencies continue their efforts to improve the physical security of critical HV transformer substations, Congress may consider several key issues as part of its oversight of the sector.

---

http://www.bpa.gov/Finance/FinancialPublicProcesses/CapitalInvestmentReview/2014CIRDocuments/Security%20Full%20Asset%20Strategy%20Final%20Draft.pdf.

[135] BPA, February 2014, p. 31.

[136] BPA, "2nd Quarter Capital Project Status Report," May 16, 2015, p. 1, http://www.bpa.gov/Finance/AssetMgmt/CapitalProjectStatusReports/Q2-2015-External-Quarterly-Project-Status-Report.pdf.

[137] BPA, "500kV Spare Transformer Procurement," fact sheet, 2015, http://www.bpa.gov/Finance/AssetMgmt/ProjectSynopsessort/500-kV-Spare-Transformer-Project.pdf.

[138] New York Power Authority, Memorandum to the Trustees Regarding NERC CIP Version 5 Physical and Cyber Security Upgrades–Capital Expenditure Authorization Request and Contract Award, January 27, 2015.

[139] New York Power Authority, Request for Proposals No. Q14-5730RH, September 10, 2014.

[140] Corina Rivera Linares, "Pepco's Capital Expenditure Forecast for 2014-2018 Includes $157M for Three More Transmission Projects," TransmissionHub, May 7, 2015.

[141] William Gausman, Pepco Holdings, "Physical Security Electric Grid," slide presentation, Mid-Atlantic Conference of Regulatory Utilities Commissioners, June 25, 2014.

Identifying Critical Transformers

A fundamental consideration regarding HV transformer security is a clear and stable understanding of which transformers are "critical." The USA PATRIOT Act of 2001 defines "critical infrastructure" in the most general sense as "systems and assets ... so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[142] In its 2009 guidelines for identifying critical assets specifically in the electricity sector, NERC defines critical assets as those "that if destroyed, degraded, compromised (e.g., misused) or otherwise rendered unavailable would unacceptably affect the reliability or operability of the [bulk-power system] as a whole.... "[143] FERC's 2014 order mandating physical security standards for the grid defines a "critical facility" as "one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."[144] All three definitions associate "criticality" with a failure event of national significance, although none provides a more prescriptive basis for identifying such assets.

In its physical security order, FERC does not require that a "mandatory" number of critical facilities be identified under the standards.[145] Determination of whether a specific HV transformer is "critical" will be based on each individual asset owner's "objective analysis, technical expertise, and experienced judgment."[146] In its physical security standards, NERC requires transmission owners with HV assets meeting prescriptive criteria to examine whether they *may* have critical transformers, but it is up to the owners to determine themselves if any of their assets *are* critical through a periodic risk assessment based on their own respective transmission analyses, subject to independent validation.[147] Thus, grid owners could have considerable latitude in determining which of their transformer substations (if any) are critical and therefore subject to the requirements of the new standard.

Although there are many candidate transformer substations in the grid, relatively few are likely to be of national significance. As discussed above, of the numerous HV transformer substations in the United States, FERC's 2013 power flow analysis identified only 30 as being critical to the national grid (although each of these substations may contain multiple HV transformers). Whether the number of critical transformer substations under FERC's definition above turns out to be higher or lower than 30, it will likely be only a small fraction of the total asset base. This conclusion is consistent with FERC's expectation that under NERC's new standard "the number of facilities identified as critical will be relatively small.... For example, of the many substations on the Bulk-Power System, our preliminary view is that most of these would not be 'critical' as the term is used in this order."[148] Consistent with this view, the NERC working group responsible for drafting the proposed physical security standard likewise expected the number of critical

[142] P.L. 107-56 §1016(e).

[143] North American Electric Reliability Corporation (NERC), "Security Guideline for the Electricity Sector: Identifying Critical Assets," September 17, 2009, p. 1, http://www.nerc.com/fileUploads/File/Standards/Reference%20Documents/Critcal_Asset_Identification_2009Nov19.pdf.

[144] FERC, March 7, 2014, p. 3.

[145] FERC, March 7, 2014, p. 3.

[146] FERC, March 7, 2014, p. 3.

[147] NERC, CIP-014-1, pp. 24-25.

[148] FERC, March 7, 2014, p. 3.

facilities to be "small and that many Transmission Owners that meet the applicability of this standard will not actually identify any such Facilities."[149]

Although the new NERC physical security standards were approved by FERC after extensive utility and public comments, some stakeholders take issue with specific requirements and methodology in the standards. For example, some analysts have objected to NERC's standards as focusing too narrowly on a limited number of substations evaluated individually. They argue this approach fails to adequately consider potential impacts from a planned, multi-substation attack. They assert that NERC's approach may overlook transformers that are "critical" in the context of such an attack.[150] FERC has rejected these arguments (for the time being) arguing that "by protecting individual critical facilities, responsible entities will necessarily protect critical facilities against simultaneous attacks."[151] FERC states that it is not prepared "to expand the scope of covered facilities to include those not individually critical ... at this early stage of industry experience with the new requirements. Our priority at this time is to have responsible entities protect the most critical facilities."[152] However, the commission also states that it remains "open to a different approach in the future as industry continues to gain experience in this area and as risks may evolve."[153]

Properly identifying which HV transformer substations are critical is a key issue. Otherwise, the electricity sector risks the possibility of hardening too many substations, hardening the wrong substations, or both. Either outcome could increase ultimate costs to electricity consumers without commensurate security benefits, and could potentially divert limited security resources from other important grid priorities (e.g., cybersecurity). Hardening too few substations could leave the grid exposed to unacceptable levels of risk. Independent verification is intended to validate utility assessments of substation criticality, but the standard's reliance on company-by-company assessments may still allow for important differences in analytic methodology or assumptions, and thus inconsistent conclusions about transformer criticality. Furthermore, company-specific studies may not align with a "top down" assessment of asset criticality like that performed by FERC in its Electrically Significant Location (ESL) analysis. Congress may examine whether company-specific assessments of transformer criticality could differ from national-level assessments or assessments using other analytic approaches, and what implications, if any, such differences might have on overall grid security and company efforts to protect particular substations.

Confidentiality of Critical Transformer Information

Ensuring the confidentially of critical infrastructure information has been a long-standing concern across all critical infrastructure sectors. It is a key reason for the establishment of sector Information Sharing and Analysis Centers (ISACs), including the Electricity Sector ISAC, discussed above. Confidentiality also factors into the administration of the industry's spare transformer programs and other activities related to critical infrastructure. FERC has established

[149] NERC, CIP-014-1, p. 22.

[150] Foundation for Resilient Societies, Reliability Standard for Physical Security, Request for Rehearing on FERC Order No. 802, Docket No. RM14-15-000, Submitted to FERC on December 21, 2014, p. 8.

Filed by the Foundation for Resilient Societies

[151] Federal Energy Regulatory Commission (FERC), Order Denying Rehearing, Docket No. RM14-15-001, April 23, 2015, p. 5.

[152] FERC, April 23, 2015, p.5.

[153] FERC, April 23, 2015, p.5.

policies for the protection of critical energy infrastructure information (CEII) through a series of orders, beginning with Order 630, issued February 21, 2003.[154] The order (§27) defines CEII as information that "must relate to critical infrastructure, be potentially useful to terrorists, and be exempt from disclosure under the Freedom of Information Act [FOIA]." It also establishes procedures and responsibilities for determining what information qualifies as CEII and handling CEII requests.[155] FERC's 2014 order mandating physical security standards also requires procedures to ensure confidential treatment of sensitive information.[156]

Press articles in the wake of the Metcalf attacks, notably in the *Wall Street Journal*, cited specific details about FERC's 2013 ESL analysis, reportedly from a copy of a FERC presentation obtained by the paper. Notwithstanding FERC's orders on CEII, Members of Congress and FERC officials have expressed concern that the release of the presentation by FERC staff and the publication of details in the press potentially compromised grid security.[157] Others reportedly have disputed this concern, including the former FERC Commissioner responsible for commissioning and presenting the ESL study findings at industry meetings.[158] In April 2014, the DOE Inspector General issued a management alert which concluded that the FERC presentation in question "should have been classified and protected from release" and "that the Commission may not possess adequate controls for identifying and handling classified national security information."[159] The Acting Chairman of FERC testified at the time that the commission was adopting the Inspector General's recommendations to improve its handling of CEII and requested additional authority from Congress for exemption from FOIA.[160]

On January 30, 2015, the DOE Inspector General released a follow up inspection report related to the IG's earlier examination of CEII handling by FERC. The report concluded that

> the Commission's controls, processes and procedures for protecting nonpublic information were severely lacking. Specifically, we found that staff inconsistently handled and shared Commission-created analyses that identified vulnerability of the Nation's electric grid without ensuring that the data was adequately evaluated for sensitivity and classification.[161]

The IG report noted that FERC's actions to remediate its CEII lapses since the IG's earlier Management Alert were "a good start," but that additional measures were recommended.[162]

---

[154] For an overview, see Federal Energy Regulatory Commission (FERC), "Critical Energy Infrastructure Information (CEII) Regulations," web page, June 28, 2010, http://www.ferc.gov/legal//maj-ord-reg/land-docs/ceii-rule.asp.

[155] Federal Energy Regulatory Commission (FERC), Order No. 630, Final Rule, February 21, 2003, http://elibrary.ferc.gov/idmws/common/opennat.asp?fileID=9639612.

[156] FERC, March 7, 2014, p. 10.

[157] Senate Committee on Energy and Natural Resources, "Sens. Landrieu, Murkowski Ask Inspector General to Examine Leaks of Grid Vulnerabilities," press release, March 27, 2014; The Honorable Cheryl LaFleur, Chairman (Acting), Federal Energy Regulatory Commission (FERC), Testimony Before the Senate Committee on Energy and Natural Resources Hearing, "Keeping the Lights On—Are We Doing Enough to Ensure the Reliability and Security of the U.S. Electric Grid?," April 10, 2014.

[158] Bobby McMahon, "Wellinghoff Says FERC Analysis of Grid Vulnerability was Public, Calls Review 'Waste of Time'," *Inside FERC*, March 31, 2014, p. 1.

[159] U.S. Department of Energy, Office of Inspector General, "Review of Internal Controls for Protecting Non-Public Information at the Federal Energy Regulatory Commission," DOE/IG-0906, April 2014, p. 1.

[160] The Honorable Cheryl LaFleur, Testimony on April 10, 2014.

[161] U.S. Department of Energy, Office of Inspector General, (DOE/IG) "Review of Controls for Protecting Nonpublic Information at the Federal Energy Regulatory Commission," DOE/IG-0933, January 2015, p. 1.

[162] DOE/IG, January 2015, p. 6.

According to the IG, FERC's comments and additional plans in response to the new report were generally responsive to the report's findings and recommendations.[163]

FERC staff may be taking steps to improve the way CEII is safeguarded in response to the Inspector General's reports, but securing CEII may continue to be an issue if NERC's new physical security regulations are approved by the commission. NERC's regulations would require independent risk assessments by multiple grid owners and 3rd party validation of those assessments. This process, by construction, would cause considerable new CEII to be created (e.g., multiple Midwest power flow models) and shared among utilities, RTOs, and consultants in ways that may be new to the industry. Ensuring that CEII generated and transferred among these entities remains secure could require special attention. As FERC's improper management of the ESL study information shows, having strong CEII policies in the context of NERC's new physical security regulations may not guarantee that those policies will be correctly and uniformly followed—even by the agency that created them.

The Critical Electric Infrastructure Protection Act (H.R. 2271 §2(a)) would strengthen federal protections for critical electric infrastructure information. Among other provisions, the bill would exempt such information from disclosure under the Freedom of Information Act or any state, tribal, or local law requiring such disclosure. The bill would also require FERC to promulgate regulations, issue orders, provide standards, and specify sanctions to ensure appropriate sharing of critical electric infrastructure information and prevent its unauthorized release. The bill would allow federal officials to grant temporary access to classified information to key personnel of entities subject to grid security emergency measures, further discussed below.

Adequacy of HV Transformer Protection

The electric power sector has had physical security guidelines in place for well over a decade, as discussed above. These voluntary guidelines have been updated and expanded periodically to reflect industry experience, changes in the security environment, and new technologies. Prior to 2014, however, it appears that the physical security initiatives among grid owners were focused primarily on preventing vandalism and theft (of copper wire) rather than a terrorist attack.[164] As the recent substation attacks in California, Arkansas, and Florida have shown, many other security measures available to grid owners were not implemented—even at critical HV substations.

A grid owner's focus on vandalism and theft may be understandable because such incidents have occurred frequently and their associated costs are tangible and well-understood. Investing in security against a terrorist attack presents a greater challenge in terms of costs and benefits. As a 2006 report from the Electric Power Research Institute states,

> Security measures, in themselves, are cost items, with no direct monetary return. The benefits are in the avoided costs of potential attacks whose probability is generally not known. This makes cost-justification very difficult.[165]

Note that cost-justification requires not only the approval of utility management, but also of FERC and potentially state public utility commissions which regulate the rates grid owners may

[163] DOE/IG, January 2015, p. 6.

[164] See, for example, Michael Wills, "Changes at Duke Energy Substations Crack Down on Copper Thieves," *WUNC Radio 91.5*, May 22, 2013; Scott Kraus, "Hit Hard by Copper Wire Thieves, PPL Fights Back," *The Morning Call* (Lehigh, PA), June 6, 2013.

[165] Electric Power Research Institute (EPRI), *Technologies for Remote Monitoring of Substation Assets: Physical Security*, March 2006, p. viii.

charge for electric transmission and distribution service. Regulators are responsible for ensuring that electricity rates are just and reasonable. They must be convinced that any new grid security capital costs and expenses are necessary and prudent before they will allow them to be passed through to ratepayers.[166]

The Metcalf incident and GridEx exercises have provided the electric sector with valuable new information about the potential threat, vulnerability, and consequence of a coordinated attack on HV transformers. Risk assessments incorporating this information presumably would justify (with or without a new NERC standard) increased security investments at critical substations to prevent intentional attacks. The spending plans announced in 2014-2015 at PG&E, Dominion, BPA, and other utilities for HV substation security appear to reflect such risk and cost-benefit reassessments. Nonetheless, there continues to be considerable uncertainty about the risk of terror attacks on the power grid, and what measures are economically justified in addressing them. PG&E, BPA, and the other utilities announcing large security investments have already decided to make such investments. Other major owners of critical HV transformers have not publicly announced similar plans, in some cases because they have not yet completed security evaluations under NERC's new standards, so they are unsure what new measures they will require. For example, based upon a security gap analysis after the Metcalf incident, Florida Power and Light (FPL) identified multiple potential security enhancements, but has only implemented some of them; other measures have been delayed for comparison to requirements under NERC's new standards.[167]

NERC's proposed standards for power grid physical security would ensure considerable consistency in the *analytic process* utilities must undertake to identify critical substations and develop plans to secure them. However, the standard may not ensure consistency among the various security plans nor in the specific measures the individual asset owners will choose to implement to reduce the risk of intentional attacks. Apart from the physical aspects of their assets, a number of factors may lead to differences in security implementation among grid owners, including differences in organization, ratemaking, accounting, and management capability. In particular, how physical security is managed within a corporate structure can influence the effectiveness of physical security programs. For example, a 2014 corporate memo from PG&E leaked to the press states that "due to the existing structure and limited authority of CSD [Corporate Security Division], little has changed relative CSD's abilities to make significant and intended security improvements."[168] How capital is allocated and accounted for can also be a barrier to physical security implementation and verification. In a 2014 report to Florida regulators, FPL stated that

> not all security costs are contained within the Corporate Security budget. Some physical security costs are shared with appropriate operational business units. For example, the cost of security equipment for new substations is rolled into the cost of the substation. Not all physical security costs are budgeted and tracked in separate line items. Therefore, difficulties exist estimating total costs of FPL's physical security efforts.[169]

As FERC continues to implement its policy of regulating physical security of the power grid, Congress may examine whether company-specific security initiatives appropriately reflect the risk profiles of their particular assets, and whether additional security measures across the grid

[166] EPRI, September 30, 2104, pp. 24-25 and pp. 37-38.

[167] Florida Public Service Commission (FPSC), *Review of Physical Security Protection of Utility Substations and Control Centers*, December 2014, p. 31.

[168] Pacific Gas and Electric, "Recommendations for Security," memorandum, August 30, 2014, p. 1, available at https://s3.amazonaws.com/s3.documentcloud.org/documents/2081637/pg-amp-e-memo-august-30-2014.pdf.

[169] FPSC, December 2014, p. 25.

uniformly reflect terrorism risk from a national perspective. Examining the extent to which the corporate structures and accounting functions support company-specific physical security programs may be of particular interest as grid owners adapt to evolving threats and physical security requirements.

Quality of Federal Threat Information

The power industry's physical security risk assessments rely upon information about security threats provided by the federal government, among other sources, communicated through the ISAC, during DHS and other agency briefings, or through other channels. The quality and timeliness of this threat information is a key determinant of what grid owners need to be protecting against and what security measures to take. Incomplete or ambiguous threat information—especially from the federal government—may lead to inconsistency in physical security among grid owners, inefficient spending of limited security resources at facilities (e.g., that may not really be under threat), or deployment of security measures against the wrong threat. For example, prior to FERC's physical security order, the head of NERC, which initially opposed mandatory physical security standards, stated?

> I am concerned that a rule-based approach for physical security would not provide the flexibility needed to deal with the widely varying risk profiles and circumstances across the North American grid and would instead create unnecessary and inefficient regulatory burdens and compliance obligations.[170]

Differences in the interpretation or application of threat information, as discussed in the previous section, may be a reason why some large utilities have announced major new substation security initiatives while others have not.

Concerns about the quality and specificity of federal threat information have long been an issue across all critical infrastructure sectors.[171] Threat information continues to be an uncertainty in the case of power grid physical security. For example, the PJM regional transmission organization employs probabilistic models to assess risks to the grid due to equipment malfunction and severe weather, but its model has not incorporated an assessment of a physical attack due to insufficient data.[172]

Some federal officials reportedly have characterized the Metcalf incident as a domestic terrorist attack, potentially a "dry run" for a more destructive attack on multiple HV transformer substations, while the Federal Bureau of Investigation has stated that it does not believe Metcalf was a terrorist incident.[173] Because the perpetrators have not been identified, it is impossible to know for certain, but the ambiguity has significant implications for HV substation security going forward. Although there is wide consensus that the Metcalf attack was extremely serious, some industry analysts have opined that FERC's physical security order may be an "overreaction" to Metcalf.[174] By contrast, former DHS Secretary Michael Chertoff has predicted that "the

---

[170] Gerry Cauley, President and CEO, North American Electric Reliability Corporation (NERC), Letter to Senate Majority Leader Harry Reid, February 12, 2014, p. 2, http://www.nerc.com/news/Headlines%20DL/NERC%20Response%20to%20Senators%20Letter%20-Reid%20%202%2011%2014%20v4.pdf.

[171] See, for example, Philip Shenon, "Threats and Responses: Domestic Security," *New York Times*, June 5, 2003, p. A15.

[172] EPRI, September 30, 2104, p. 17.

[173] Rebecca Smith, February 5, 2014.

[174] Deborah Carpentier, "NERC Gains in Vegetation Management, Cyber and Physical Security, and Reliability Assurance," *Natural Gas & Electricity* (Wiley Periodicals), May 2014, p. 31, http://www.crowell.com/files/NERC-

sophistication and resulting damage of the Metcalf attack will ... be exceeded" in a future attack.[175] Still others have expressed concern that FERC's physical security concerns may be too heavily focused on another Metcalf-type scenario (the last threat) rather than a wider range of potential future threats (the next threat).[176]

There is widespread agreement among government, utilities, and manufacturers that HV transformers in the United States are vulnerable to terrorist attack, and that such an attack potentially could have catastrophic consequences. But the most serious, multi-transformer attacks could require acquiring operational information and a certain level of sophistication on the part of potential attackers. Consequently, despite the technical arguments, without more specific information about potential targets and attacker capabilities, the true vulnerability of the grid to a multi-HV transformer attack remains an open question. As Congress seeks to establish the best policies to address HV transformer vulnerability relative to other infrastructure security priorities, understanding this vulnerability in the context of specific demonstrable threats may become increasingly important. To this end Congress may examine how federal threat information is developed and used by grid owners, and how limitations and uncertainty of this information may affect the HV transformer physical security among electric utilities.

Recovery from HV Transformer Attacks

Physical security for HV transformer substations has the primary purpose of preventing successful attacks against these critical assets within the power grid. However, in the event of a successful attack, measures to minimize its effect on the overall grid are equally important so that the loss of any particular transformer remains a local event. To this end the electric power industry emphasizes its strategy of "defense-in-depth," which includes incident response and recovery in addition to preparation and prevention.[177] Industry initiatives to enhance grid resiliency, including incident recovery programs such as the DHS recovery transformer program and EEI's spare transformer program, contribute to the power grid's ability to sustain a terrorist attack without widespread grid failure. Indeed, some analysts have pointed to the Metcalf incident as a successful demonstration of grid resiliency; electric service was not interrupted despite the loss of a critical substation in the San Francisco Bay area. Nonetheless, some policymakers have proposed additional federal authorities to respond to physical incidents affecting grid critical infrastructure, including HV transformers.

Some stakeholders, including FERC officials, have asserted that the commission's current grid reliability authority under the Federal Power Act (§215) does not provide FERC with adequate authority for emergency action in the event of an attack on the grid. A House bill to amend the Federal Power Act with respect to critical electric infrastructure security (H.R. 2271) would allow the President to authorize the Secretary of Energy to order emergency measures to protect grid reliability during a "grid security emergency" (§(b)(1)). The director of FERC's electric reliability office has testified in support of the bill that FERC's existing "procedures ... for the development and approval of reliability standards do not provide an effective and timely means of addressing urgent cyber or other national security risks to the bulk power system."[178] NERC's president

Gains-in-Vegetation-Management-Cyber-and-Physical-Security-and-Reliability-Assurance.pdf.

[175] Michael Chertoff, "Building a Resilient Power Grid," *Electric Perspectives*, May/June 2014, p. 35.

[176] Edison Electric Institute, briefing for the Congressional Research Service, February 23, 2014.

[177] Edison Electric Institute, "The Electric Power Industry's Commitment to Protecting Its Critical Infrastructure," February 2014, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Critical_Infra_Physical_Protection.pdf.

[178] Michael Bardee, Director, Office of Electric Reliability, Federal Energy Regulatory Commission, Testimony before

likewise has testified that he generally supports legislation clarifying federal authority during grid emergencies, as long as they focus clearly on "national, catastrophic instances" and do not conflict with the existing system of ongoing measures in place to protect the grid.[179] Utility industry representatives also support facilitation of industry-government coordination in the event of an attack on the grid.[180] As consideration of H.R. 2271 or similar legislation continues, Congress may focus on specific language related to consultation, duration of emergency measures, grid recovery activities, and other details to ensure that they align with a complex industry structure while achieving the bill's objectives in the event of a future security incident.

As discussed above, the DOE's *Quadrennial Energy Review* calls for federal efforts to develop one or more critical HV transformer reserves. H.R. 2244 would mandate a DOE plan for how such a reserve program could be carried out. Some in the utility industry support the policy intentions of such a reserve, as already demonstrated by the industry's own spare HV transformer programs and planned expansion of those programs, but they believe stakeholders "will be better served by allowing the industry to create the structure, cost responsibility and pricing for [transformer] sparing services as opposed to a top-down government solution."[181] They believe federal assistance would be most helpful if limited to funding the startup of a transformer reserve program administered by the asset owners themselves. The Grid Assurance sparing service appears consistent with a private sector-driven approach to expand existing spare transformer initiatives.

Others have questioned the cost-effectiveness of a new national HV transformer reserve program, asserting that—had it been in place—the reserve program envisioned by H.R. 2244 would not have been called upon by any grid incident over the last ten years.[182] As Congress considers any plans for a federally administered strategic transformer reserve, it may consider the relationship of such a program to ongoing industry efforts to maintain HV transformer spares, the relationship between federal and state administrators of such a program, its cost-effectiveness, and its practical requirements (e.g., size, location, and transportation).

Electric Grid Resilience

In addition to measures focused on the protection of critical HV transformers from physical attack, analysts have advocated policies to reduce the criticality of individual HV assets by enhancing the overall "resiliency" of the electric power grid. As a report from the Executive Office of the President states,

> Grid resilience ... includes hardening, advanced capabilities, and recovery/reconstitution. Although most attention is placed on best practices for hardening, resilience strategies must also consider options to improve grid flexibility and control. Resilience includes reconstitution and general readiness such as pole maintenance, vegetation management, use of mobile transformers and substations, and participation in mutual assistance groups.[183]

---

the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, pp. 7-8.

[179] Gerry Cauley, May 19, 2015, p. 7.

[180] Thomas A. Fanning, Southern Company, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, May 19, 2015, p. 1.

[181] Thomas A. Fanning, May 19, 2105, pp. 14-15.

[182] Gerry Cauley, Testimony before the House Committee on Energy and Commerce, Subcommittee on Energy and Power, transcript, May 19, 2015.

[183] Executive Office of the President, *Economic Benefits of Increasing Electric Grid Resilience to Weather Outages*,

A number of federal, state, and industry initiatives exist to address various aspects of electric power grid resiliency. While many of these initiatives have been motivated by weather-related events such as the Northeast Blackout of 2003 and electric grid failure during Superstorm Sandy, policies to improve grid resilience also have benefits in the context of intentional physical attacks. For example, an official from PJM has reportedly stated,

> You can only harden a substation so much. If someone wants to attack a substation, they will.... That leads us to the resilience piece. Maybe the best way to make a substation less critical is to build more transmission. A substation is critical basically because we're pushing too much power through it.[184]

Grid scale energy storage, distributed generation, smart grid technology, and other measures to redistribute or optimize transmission system power flows may also increase grid resiliency and reduce vulnerability to physical security threats.

The Enhanced Grid Security Act of 2015 (S. 1241) would require the Secretary of Energy develop an advanced energy security program to increase the "functional preservation" of the electric grid in the face of both natural and human-made threats and hazards (§7(b)). The objectives of the program would explicitly include both "security and resiliency" through vulnerability assessment, modeling, exercises, research, and technical assistance (§7(c)). The Grid Modernization Act of 2015 (S. 1243) would likewise encourage greater grid resilience, including modelling, research, and investment in grid modernization and new technologies—including tools to increase physical security (§101(3)(E)). Other legislation related to power grid resilience or efficiency would also likely have physical security implications. As Congress continues its examination of physical security policy, maintaining an integrated perspective on prevention, recovery, and resilience may help to promote an effective balance among industry investment, regulatory requirements, and federal oversight.

Author Information

Paul W. Parfomak
Specialist in Energy and Infrastructure Policy

Disclaimer

August 2013, p. 12.

[184] Mike Kormos, PJM, as quoted in "Physical Security Cure: More Transmission?," *RTO Insider*, July 1, 2014.